

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30.				1. REQUISITION NUMBER A21986093		PAGES 1 OF (1) PAGE(S)	
2. CONTRACT NO. GS-35F-0119Y		3. AWARD/EFFECTIVE DATE 09/11/2019		4. ORDER NUMBER 47QFDA19F0027		5. SOLICITATION NUMBER	
6. SOLICITATION ISSUE DATE		7. FOR SOLICITATION INFORMATION CALL:		a. NAME		b. TELEPHONE NUMBER (No Collect Calls)	
8. OFFER DUE DATE/ LOCAL TIME		9. ISSUED BY Francine L Hemphill 301 7TH ST SW WASHINGTON, DC 20024-0001 United States (b) (6)		10. THIS ACQUISITION IS UNRESTRICTED <input type="checkbox"/> SET ASIDE. % FOR <input type="checkbox"/> SMALL BUSINESS HUBZONE SMALL BUSINESS <input type="checkbox"/> 8(A)		11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED Destination <input type="checkbox"/> 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	
12. DISCOUNT TERMS NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS		13b. RATING		14. METHOD OF SOLICITATION			
15. DELIVER TO Huy Le 1800 F Street, NW Washington, DC 20405 United States (b) (6)		16. ADMINISTERED BY Francine L Hemphill (b) (6)					
17a. CONTRACTOR/ OFFEROR (b) (6) CARAHSOFT TECHNOLOGY CORP. 11493 SUNSET HILLS RD RESTON, VA 201905230 United States (b) (6)		18a. PAYMENT WILL BE MADE BY General Services Administration (FUND) The contractor shall follow these Invoice Submission Instructions. The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).					
17b. <input type="checkbox"/> CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED					

19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
ITEM NO.	TASK ITEM DESCRIPTION		PREVIOUS MOD AMT	MOD CHANGE AMT	NEW MOD AMT
0001	Base Configuration		\$0.00	(b) (4)	(b) (4)
0002	Travel		\$0.00	\$50,000.00	\$50,000.00

BPA Call Order 1 under Quality Services Management Office (QSMO) NewPay BPA

This award is in support of the The Office of Shared Solutions and Performance Improvement (OSSPI) for configuration of the SaaS solution to a government-wide baseline for Payroll.

Carahsoft Technology Corporation's technical and price quote dated August 6, 2019 in response to solicitation ID11190033 are accepted as to all items.

The period of performance for this Call Order 1 will be a 1-year base period with no options as follows: Base: 09/11/2019 - 09/10/2020

Funds are obligated to the base year on a T&M/LH basis as follows:
CLIN 0001 Baseline Configuration - (b) (4)

Funds are obligated to the base year on a CR basis as follows:
CLIN 0002 Travel - \$50,000

Total Base Year Obligated Amount: (b) (4)

25. ACCOUNTING AND APPROPRIATION DATA 285F.Q11FA000.AA20.25.AF151.H08...		26. TOTAL AWARD AMOUNT (For Govt. Use Only) (b) (4)	
---	--	--	--

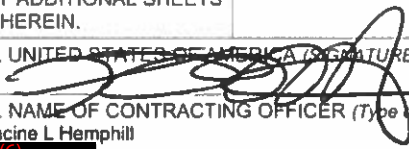
☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 and 52.212-5 ARE ATTACHED. ADDENDA ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ATTACHED.

28. CONTRACTOR IS NOT REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE.

☐ CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

29. AWARD OF CONTRACT: REFERENCE OFFER DATE YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR (b) (6)		31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) 	
30b. NAME AND TITLE OF SIGNER (Type or print) (b) (6)	30c. DATE SIGNED 9/11/2019	31b. NAME OF CONTRACTING OFFICER (Type or print) Francine L Hemphill (b) (6)	31c. DATE SIGNED
32a. QUANTITY IN COLUMN 21 HAS BEEN		32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE	
		32c. DATE	

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT
37. CHECK NUMBER		38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		40. PAID BY	
41b. SIGNATURE		42a. RECEIVED BY <i>(Print)</i>	
41c. DATE		42b. RECEIVED AT <i>(Location)</i>	
AND TITLE OF CERTIFYING OFFICER GSA Finance Customer Support		42c. DATE REC'D <i>(YY/MM/DD)</i>	42d. TOTAL CONTAINERS
1693-7227 FOR LOCAL REPRODUCTION		SEE REVERSE SIDE FOR OMB CONTROL NUMBER AND PAPERWORK BURDEN STATEMENT	
		STANDARD FORM 1449 (REV. 4-2002) Prescribed by GSA - FAR (48 CFR) 53.212	

TASK ORDER

NewPay SaaS Solution Procurement

In support of:

General Services Administration (GSA)

The Office of Shared Solutions and Performance Improvement (OSSPI)

Quality Services Management Office (QSMO)

B.1 BRIEF DESCRIPTION OF SUPPLIES OR SERVICES

The Office of Shared Solutions and Performance Improvement (OSSPI) within the Office of Government-wide Policy (OGP) of GSA has a requirement to modernize the Payroll and Work Schedule and Leave Management (WSLM) ecosystem. This Task Order (TO) will lead to a Baseline Configuration for Payroll and will include activities such as: Project Management, Analysis, Design, and Configuration. The Contractor shall perform in accordance with the terms and conditions outlined in the resultant TO and all Sections of the Blanket Purchase Agreement (BPA).

B.2 SERVICES, PRICES/COSTS, AND PERIOD OF PERFORMANCE

The Contract Line Item Numbers (CLINs) contain a hybrid contract type including:

1. Time and Material/Labor hour (T&M/LH)
2. Cost Reimbursement for Travel
2. This task order will be awarded under the established BPA.
3. The prices set forth in this Section will cover a contract period of 12 months. All deliverables under this TO are due no later than the last day of the period of performance.
4. For the T&M/LH CLIN's, the labor mix and level of effort shall not exceed funding allocated for the exercised period of performance. The contractor may reallocate, with prior written approval of the Contracting Officer's Representative (COR), the number of hours by labor category within the labor CLIN as needed to effectively manage the project, provided the total funded labor cost and total hours are not exceeded. Any additional labor categories or increases to total hours or increases to ceilings required during performance must be approved by the Contracting Officer (CO) and added to the TO by modification.
5. Long-Distance Travel (other direct costs) incurred may be burdened with the contractor's indirect rates in accordance with the contractor's disclosed practices and consistent with Federal Travel Regulation, provided that the basic contract does not prohibit the application of indirect rates on these costs.
 1. If no indirect rates are allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
 2. If no rate is specified in the schedule of prices below, no indirect rate shall be applied to or reimbursed on these costs.
6. The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices.
7. The Government will issue an Order based on the work described herein, to include the attachments.

B.2.1 CARAHSOFT T&M/LH

CLIN	Description of Services	Total Not To Exceed Cost
0001	Baseline Configuration	(b) (4)
Total		

Total T&M/LH: (b) (4)

Description	Est.# of Hours	Hourly Rates	Total
Project Manager	960	(b) (4)	(b) (4)
Sr. Program Analyst	480		
Mid Program Analyst	1440		
Jr. Program Analyst	2400		
Sr. Functional Analyst	480		
Developer Sr.	1920		
Developer Mid	1920		
Developer Jr.	3840		
Tester Mid	3840		
Solutions Architect	480		
System Engineer Sr.	960		
System Engineer Mid	1920		
Security Analyst Sr.	1920		
Security Analyst Mid	1920		
Database Architect	1920		
ETL Developer	1920		

B.2.2 CR 9/11/2019 – 9/10/2020

CLIN	Description of Services	Total Not To Exceed Cost
0002	Travel	\$50,000
TOTAL		\$50,000

Total CR: \$50,000

Total Cost of CLIN 0001 + CLIN 0002: (b) (4)

THE NTE CEILING AMOUNT REPRESENTS THE MAXIMUM AMOUNT OF THE GOVERNMENT'S LIABILITY, THE CONTRACTOR EXCEEDS THE CEILING AT ITS OWN RISK.

B.3 ADVANCED UNDERSTANDING

B.3.1. TRAVEL

Total expenditures for travel incurred in direct performance of this contract shall not exceed \$50,000 for travel during the Base Period without the prior written approval of the Contracting Officer. The Contractor shall notify the Contracting Officer in writing when travel expenditures

have reached or exceeded 70% of the contract (or each CLIN) travel expenses. Cost must be consistent with Federal Acquisition Regulations (FAR) 52.247-63 – Preference for U.S. Air Flag carriers and Federal Travel Regulation (FTR).

The contractor shall notify the COR via email at least 10 workdays prior to travel to obtain COR approval.

B.3.2. SUBCONTRACT

Prior written consent from the CO in the form of Contracting Officer Authorization (COA) is required for any subcontract that:

1. Is of the cost-reimbursement type; or
2. Is Fixed-Price and exceeds \$150,000 or 5% of the total estimated cost of the Contract, whichever value is greater.

The contractor shall submit subcontracting request to the CO via email at least 10 workdays prior to entering into any subcontracting arrangement in order to review and determine authorization, pursuant with FAR Clause 52.244-2, Subcontracts. After receiving written consent of the subcontract by the CO, the Contractor shall provide a copy of the signed, executed subcontract/consulting agreement to the CO. Note: Consulting services are treated as subcontracts and subject to the ‘consent to subcontract’ provisions set forth in this Article.

C.1 INTRODUCTION

In the early 2000s, the Federal Government launched the e-Payroll initiative to streamline payroll processing Government-wide. The initiative resulted in reducing the number of agencies that provided payroll services from 26 to the establishment of the following four approved Federal Government Payroll Shared Services Providers (SSPs):

1. Department of Defense (DoD), Finance and Accounting Service (DFAS);
2. United States Department of Agriculture (USDA), National Finance Center (NFC);
3. Department of the Interior (Interior), Interior Business Center (IBC); and
4. General Services Administration, Payroll Services Branch (GSA-PSB).

Additionally, the Department of State (State) has been permitted to continue independent payroll operations to support overseas civilian employees. The Shared Services Providers and the Department of State serve approximately 2.3 million employees globally using a range of IT systems, including internally developed and maintained software and commercial-off-the-shelf (COTS) products. The SSPs operate independent systems in disparate environments and in centers located throughout the continental US.

The Federal Government pays over 2 million federal employees every two weeks, on time, and at a relatively low cost. Some of the systems running today are in their fourth decade of operation and lack the ability to adapt to address the ever evolving legislative changes. They also lack common data or interoperability standards, common self-service and mobile features readily available in industry payroll systems that increase efficiency and customer service.

C.1.1 PURPOSE

The purpose of this TO is to configure Software as a Service (SaaS) solutions for Payroll, which will allow the government to have baseline solution that can pay over 85% of the employees serviced by the four federal payroll providers. Additional information on the longer term strategy for IT solutions can be obtained by reviewing the President's Management Agenda (PMA) and Cross Agency Priority (CAP) Goal #5.

C.1.2 AGENCY MISSION

For more than half a century, GSA has carried out a mission of servicing other Federal agencies by providing superior workplaces, quality acquisition services, and expert business solutions. The Vision of NewPay is to improve the execution and cost efficiency of Federal payroll management and continually modernize the payroll ecosystem through the collaborative efforts of Federal shared services payroll providers and SaaS vendors, while further maximizing opportunities to improve customer satisfaction.

The Federal Government recognizes the need to modernize the civilian Government payroll ecosystem. The e-Payroll initiative condensed the number of payroll providers from 26 to the four Federal SSPs currently providing payroll services as well as the Department of State. Over the last decade, there have been no significant investments to modernize legacy payroll applications. Some of the payroll systems are in their fourth decade of operation. These aging legacy systems will become increasingly more costly to maintain. The ever evolving and escalating cyber threat, the integration of modern IT infrastructure, and the inability to utilize current security best practices, including data encryption and multi-factor authentication, make legacy systems vulnerable to malicious cyber activity. Additionally, lack of data and interoperability standards, along with clearly defined policies and regulations, leads to long lead times for government-wide implementation of major policy changes impacting payroll. Furthermore, lack of interoperability also requires significant efforts and manual processes for employee and agency transfers between shared services providers.

Moreover, there is significant customer demand for consistent user experience including modern graphical user interfaces (GUI), increased interoperability, and accessibility. Finally, the legacy applications are not cost effective to maintain, and sufficient reserves have not been established for ongoing modernization and enhancements to legacy applications.

C.2 SCOPE

Over time, NewPay will modernize Payroll and WSLM systems for the four SSPs listed in Section C.1. The scope of this acquisition is to configure the SaaS solution to a government-wide baseline for Payroll.

C.3 CONFIGURATION

C.3.1 PROJECT MANAGEMENT

C.3.1.1 PROJECT MANAGEMENT STANDARDS

The Contractor shall provide project management support which includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a Project Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.3.1.2 PROJECT MANAGEMENT PLAN

The Contractor shall develop a Project Management Plan (PMP) (to include schedule, scope, risk, procurement, cost, communications/stakeholder engagement, and quality). The Contractor will use the USSM M3, PMBOK, and Agile methodologies to inform its development of the

Project Management Plan, using each as a guideline to develop its tailored methodology to achieve project success and be in accordance with Section F – Deliverables and Milestones. The Project Management Plan shall:

1. Lay out the Contractor's approach, timeline, and tools to be used in execution of this TO;
2. Take the form of both a narrative and graphic formats that display the schedule, milestones, risks, roadmaps, release plans, and resource support;
3. Include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the TO; and
4. Include in the initial draft for COR review/comment and CO final approval.

The Contractor shall update and maintain the COR approved PMP. The contractor's PMP shall include the following:

1. Describe the proposed management approach;
2. Include milestones, tasks, and subtasks required in this TO and

Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.

1. Include the contractor's Quality Assurance Surveillance Plan (QASP).
2. Include Independent Validation and Verification (IV&V) Plan
3. Include Data Management Plan

Data management plan shall address the Contractor's approach, methods, data descriptions, data organization, data storage (methods, mediums, access), data access (roles, methods, software, privacy and confidentiality) and archiving to maintain employee payroll data.

1. Include Test Plan

Test plan should include the testing strategy, approach, objectives, testing methods, roles and responsibilities, results and defect/error logging, defect/error criticality rating, resolution, and reporting.

C.3.1.3 PROJECT REPORTING

C.3.1.3.1 COORDINATE A PROJECT KICKOFF MEETING

The contractor shall schedule, coordinate, and host a Project Kickoff Meeting within 14 days after TO award at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, key GSA personnel, and other relevant Government personnel, the CO and the COR. The contractor shall provide the following at the Kickoff Meeting:

1. Draft Project Management Plan (PMP) (Final PMP is due within 30 days after TO award), and
2. Draft Quality Assurance Surveillance Plan (QASP) Plan (Final QASP is due within 30 days after TO award).

C.3.1.3.2 PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the PM, COR, CS, and the CO.

The MSR shall include the following:

1. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status (security clearance, etc.).
4. Government actions required.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
7. Accumulated invoiced cost for each CLIN up to the previous month.
8. Projected cost of each CLIN for the current month.

C.3.1.3.3 CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a Monthly Technical Status Meeting with the COR, CO/CS and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide draft minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned to the COR, and CO/CS within five workdays following the meeting for COR, and CO/CS review via email. The contractor PM shall make any updates requested for CO/CS final approval and submission to the ITSS system.

C.3.1.3.4 PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The contractor shall keep a summary of all long distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.3.2 ANALYSIS AND DESIGN

The Contractor shall perform Analysis and Design for the SaaS solution to support the configuration requirements identified in Section C.3.3.

C.3.2.1 FIT-GAP

The Contractor will conduct a fit-gap analysis, with Government Subject Matter Experts, comparing the SaaS solution capability to Attachment A - Business Capabilities and Data Standards, Attachment B - Technical Capabilities, the Pay Plans listed in Attachment C - Pay Plans, Attachment D - Interface Requirements, the standards in Attachment F - Data Standards, Attachment I - Functional Requirements, and Attachment H - Security Requirements. The government will provide the data and pay outputs of legacy payroll processing for testing.

C.3.2.2 BUSINESS RULES

There are a multitude of business rules associated with the various pay plans (See Attachment C - Pay Plans), employee types, leave codes, and other factors that impact Payroll. The Contractor will document the business rules for payroll and reporting to configure the solution(s). The Contractor will record and document the business rules in an agreed upon format. Each business rule will be traceable to a statute, policy, regulation, and/or technical and business capabilities (see Attachment A - Business Capabilities and Data Standards, Attachment B - Technical Capabilities).

C.3.2.3 AGENCY SECURITY REQUIREMENTS

The Contractor shall comply with the additional security capabilities listed in the Security tab in Attachment H - Agency Security Requirements and any associated security requirements identified during analysis and design.

C.3.3 PAYROLL CONFIGURATION

The Contractor shall configure the SaaS payroll to achieve the capabilities in Attachment A - Business Capabilities and Data Standards, Attachment B - Technical Capabilities, the Pay Plans listed in Attachment C - Pay Plans, Attachment D - Interface Requirements, the standards in Attachment F - Data Standards, Attachment I - Functional Requirements, and Attachment H - Security.

The capabilities, requirements and reference data for configuration are in the attachments listed below:

Description	Attachment	Reference location
Business Capabilities and Data Standards	A	BPA Payroll Business Capabilities Tab
Technical Capabilities	B	BPA Payroll Activities Only
Pay Plans	C	Task Order 1
Interface Requirements	D	Task Order 1
Reserved	E	
Data Standards and Architecture	F	Task Order 1
Standard/Status- Monthly Reports	G	Task Order 1
Agency Security Requirements	H	Task Order 1
Functional Requirements	I	Task Order 1

C.3.3.1 CONFIGURATION MANAGEMENT

Configuration management applies to the configuration of the SaaS solution to meet the requirements for timely and accurate processing and calculations. The Contractor will ensure the Configurations are based on statute, policy, or regulation and are traceable to the authorizing rules. The Contractor will provide a crosswalk to trace each of the configurations (elements of the configuration) to the applicable statute, policy, regulation, and group or category of employees (e.g. pay-plan, occupational series, agency). The Contractor shall document and record Configurations. The Contractor shall maintain Configuration documentation on current, planned and historical configurations including performance, functional, and physical attributes with requirements, design, and operational information.

C.3.4.2 TESTING

Testing is an integral and essential step. The Contractor will develop, maintain, and execute a test plan that demonstrates an approach and methodology to ensure the accuracy of payroll calculations (gross, net, deductions, contributions, leave, etc.), the cogency of the processes, and the validity of the timing. The Contractor shall prioritize resolution activities, address any configuration issues, and identify any additional data validation and verification efforts.

The Contractor shall perform system regression testing to validate configurations. The Contractor shall report regression testing results to the COR and correct the resulting errors.

The Contractor shall develop and execute test cases to determine the accuracy and efficacy of the results of the Contractor's solution compared to the Government's current system. The Contractor will provide the results of the test cases for Government evaluation.

The Contractor shall maintain a test defect log with the capability to record, prioritize, track and report issues, errors, and defects discovered throughout the implementation and PoP. The Contractor shall address and correct identified errors and results. The log shall be available to the Government for review.

The Contractor shall validate Payroll SaaS results against policies, regulations, and standards as well as Government payroll data to prove the configurations. Validation will include the processing of Payroll data in an environment that mirrors the production environment. It will include the comparison of results between the test data and SaaS solutions.

The Contractor shall review the differences in the results to determine the cause(s) of the differences and provide their findings to the government for evaluation and validation. The Contractor shall make the appropriate corrections to align the results and eliminate differences in results between the test data and SaaS solutions.

Where discrepancies are noted, the Government will validate the results against the requirements and make a determination on how to proceed. Where the Government determines the SaaS calculation is correct, the COR will work with the appropriate government organizations/representatives regarding the differences in the results. In cases where the interpretation of requirements are not clear or agreed upon, the Government will obtain clarification from the regulatory authority.

C.3.5 DATA INTEGRATION AND DATA INTEROPERABILITY

The Contractor shall provide interfaces to those entities identified in Attachment D - Interface Requirements. Those entities and their outputs include tax information the IRS, SSA, State, county, and local taxing authorities; non-federal retirement plans; health and life insurance providers; and unions and associations member dues and others.

The Government will operate a data integration platform to facilitate the exchange of data between the legacy solutions and SaaS solutions. The Contractor shall implement standard Application Program Interfaces (APIs) and develop APIs (as required) to the Government Data Integration Platform and enable interoperability of inbound/outbound APIs through the Government Data Integration Platform. The Contractor shall identify record, validate, and identify each discrete interface to/from the Contractor's SaaS solution.

Where the Government determines the data integration platform is not the most efficient and/or effective transfer method, the COR will work with the Contractor to determine the most effective method. The Contractor shall propose solutions to support the data conversion and transfer to the Contractor's SaaS product.

C.4 SECURITY

The Contractor shall meet all security requirements as they pertain to the Cloud SaaS FedRAMP ATO and the GSA specific ATO including all related integrations and connections - Reference Attachment H.

C.4.1 CLOUD SAAS FEDRAMP ATO

As indicated in the Security tab in Attachment H - Technical Capabilities, the Contractor shall obtain a FedRAMP Authority to Operate, at the moderate level, for its solutions within one year of the BPA award date and it shall be maintained in good standing for the duration of the BPA. No substitutions or waivers will be granted to replace FedRAMP authorization.

The Contractor shall ensure compliance with Federal Risk and Authorization Management Program (FedRAMP) within one year of BPA award and prior to migration of production personnel and payroll data to the solution and prior to the conduct of processing payroll and WSLM in parallel with legacy systems (parallel processing). FedRAMP compliance includes:

1. Authorization Planning and Security Package Development;
2. Identify AO Specific Requirements and Controls;
3. Complete FedRAMP Application and engage third-party assessment organization (3PAO);
4. Coordinate w/3PAO in completion of FedRAMP Security Assessment Plan (SAP)/ Security Assessment Report (SAR)/ Plan of Action and Milestones (POA&M);
5. Continuous Monitoring; and
6. Complete Monthly Continuous Monitoring Deliverables.

The Contractor shall comply with the additional security requirements for FedRAMP authorization in Attachment H - Agency Security Requirements, *Section 2 - Cloud Information Systems – IT Security and Privacy Requirements*.

C.4.2 GSA SPECIFIC ATO FOR FEDRAMP LEVERAGING

The Contractor shall comply with agency security requirements to achieve and maintain an Authority To Operate (ATO) by addressing the FedRAMP Customer Responsible Controls for agency implementation of the payroll SaaS solution. The Contractor shall also comply with agency security requirements as they pertain to any connections or integrations to and from the SaaS product. The security requirements for GSA are in Attachment H (Agency Security

Requirements). The Contractor shall comply with the additional security capabilities listed in the Security tab in Attachment B - Technical Capabilities.

C.4.3 FEDERATED IDENTITY AND ACCESS MANAGEMENT

The Contractor shall document and configure security for user roles and user access (Access Management) Validate the configuration and controls with customer Functional SMEs (and Technical SMEs) to validate requirements.

The Contractor shall develop and implement role-based access or security configurations for user roles and user access at the appropriate level, as determined by the Government, for retrieving, transferring, and accessing data protected by Federal and agency-level privacy mandates (e.g., health, EEO, garnishments).

C.4.4 IPv6

The Contractor shall provide complete support for IPv6 within the SaaS solutions provided.

D.1 PACKAGING, MARKING AND SHIPPING

All deliverables submitted to the Government shall indicate the contract number, TO number, contractor's name, description of items contain therein and the consignee's name and address for which the information is being submitted. The contractor shall follow the marking requirements specified by the Government.

All reports and deliverables should be submitted electronically in accordance with Section F.5 of this task order.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work required under this TO shall be performed by the Contracting Officer Representative (COR), or other individual as designated by the CO.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the TO. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this contract (ID11190033), the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires

additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

Note: Specific inspection/acceptance criteria required for this solicitation are outline are outlined in GSAM 552.246-72 Final Inspection and Tests (Sep 1999).

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have 10 workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government will provide written notification of acceptance or rejection of all final deliverables within 15 workdays unless specified otherwise. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected by the contractor within 15 workdays of the rejection notice. If the deficiencies cannot be corrected within 10 workdays, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within 10 workdays.

For T&M/LH –

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services and enter into discussions with the Contractor to determine how the government can be made whole.

For CR –

If the contractor does not provide travel receipts that conform to the requirements of this Award and adhere to the joint federal travel regulations, the Government will not reimburse travel.

E.3.7 ACCEPTANCE OF IT DEVELOPMENT REQUIREMENTS

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

F.1 TASK ORDER PLACE AND PERIOD OF PERFORMANCE

The place of performance will be at the Contractor's facility. The period of performance for this TO is a 1-year base period from the date of the award.

F.2 DELIVERABLES

The following schedule of milestones will be used by the CO and COR, to monitor timely progress under this request. The contractor shall provide the required deliverables based on the schedule identified below and in Section C in the required format to the CS, CO, PM, COR, and ITSS on the specified dates. Below are the required deliverables and the specified dates:

Deliverables Table

Item#	Ref	Description	Success Criteria	Deliverable Due Date
C.3.1 Project Management				
1	C.3.1.2	Project Management Plan	Taking relevant inputs from the project stakeholders, the plan contains detailed information about the project, including subsidiary project management plans and related project planning documents. Defines the roles of members in the project team, tasks that will be undertaken by each team member and specific time period within which the team member has to complete the assigned task. The comprehensive plan should be detailed enough to be referred to by the project team and stakeholders for decision making and also for clarification on ambiguous areas.	Within 30 days of contract award

2	C.3.1.3	Quality Assurance Surveillance Plan	<p>The plan identifies each area requiring quality control and the quality related means and standards against which it will be measured and assured. The plan also outlines the means by which each quality event will be documented. Appropriate goals are identified with deadlines for re-measurement when not attained. Contingencies for repeated quality failures are identified. The plan identifies why quality assurance is performed, what is being tracked, who is responsible for quality assurance, how to perform measurements, how to document progress in areas being monitored, including improvements implemented as a result thereof, and the process for updates of quality control procedures and quality assurance measures, including the plan to avoid those quality errors in the future. The QASP is updated within 10 days of any changes to quality controls.</p>	Within 30 days of contract award
---	---------	-------------------------------------	--	----------------------------------

3	C.3.3.1.4.	Project Kickoff Meeting	<p>The Contractor shall conduct a KickOff Meeting</p> <p>Contractor provides at the kickoff meeting:</p> <p>a. Draft Project Management Plan to include: The proposed management approach; Milestones, tasks, and subtasks required in this TO and Provides for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations; Independent Validation and Verification (IV&V) Plan Data Management Plan Test Plan</p> <p>b. Draft Quality Assurance Surveillance Plan (QASP).</p>	14 days after TO award
4	C.3.3.1.4.1	Project Kickoff Meeting Minutes	Draft meeting minutes provided within 10 days of the meeting include attendees and roles, topics discussed and follow-up action items.	14 days after Kickoff Meeting

5	C.3.1.3.2	Monthly Status Report (MSR)	<p>Report is provided by the tenth of each month via electronic mail to the COR and the CO. The MSR includes:</p> <ul style="list-style-type: none"> a. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task. b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them. c. Personnel gains, losses, and status (security clearance, etc.). d. Government actions required. e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each). f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period). g. Accumulated invoiced cost for each CLIN up to the previous month. h. Projected cost of each CLIN for the current month. 	10th of every month
6	C.3.1.3.3	Technical Status Meeting Notes	Report includes attendance, issues discussed, decisions made, and action items assigned.	5 working days following technical status meeting
7	C.3.1.3.4	Trip Reports	Contains a summary of all long distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.	Within 5 days of end of travel

C.3.2 Analysis and Design				
8		Fit-gap tracking analysis results.	Documents results of contractor-performed fit-gap analysis of the payroll requirements comparing the SaaS solution capability to the test data.	IAW the Project Management Plan (PMP)
9	C.3.2.2	Business Rules Requirements Traceability Matrix	Documents the business rules for payroll to configure the solution(s), recorded and documented in the agreed upon format. Allows for each business rule to be traceable to a validated statute, policy, regulation, or technical and business capability requirements.	IAW the Project Management Plan (PMP)
C.3.3 Payroll Configuration				
10	C.3.3	Solution Configurations	Solution configured to meet the government wide and agency specific requirements. The configuration describe the grouping of the configurable elements within the SaaS solutions and their values.	IAW the Project Management Plan (PMP)
11	C.3.3.1	Configuration Management	Documents the solution's ability to meet the requirements for timely and accurate processing (of payroll) for a group or category of employees (e.g. pay-plan, occupational series, agency). Documents how the Contractor will ensure the configurations are based on statute, policy, or regulation and are traceable to the authorizing rules.	IAW the Project Management Plan (PMP)
12	C.3.3.2	Testing documentation and results	Results and defect/error logging, defect/error criticality rating, resolution, and reporting.	IAW the Project Management Plan (PMP)

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this request. The Government reserves the right to treat non-conforming markings in accordance with FAR clause at 52.227-14 subparagraphs (e) and (f).

F.3 PUBLIC RELEASE OF TASK ORDER DOCUMENTS REQUIREMENT

The contractor agrees to submit, within 10 workdays from the date of the CO's execution of the initial TO award, or any modification to the award (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (Section F).

The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the TO requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

The COR will consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.4 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the HUD OCIO designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- | | | |
|----|--------------|--|
| a. | Text | Microsoft (MS) Word, Google Docs, Portable Document Format (PDF) |
| b. | Spreadsheets | MS Excel, Google Sheets |
| c. | Briefings | MS PowerPoint, Google Slides |
| d. | Drawings | MS Visio, Google Drawings |

- e. Schedules MS Project, Smartsheet

F.5 PLACE(S) OF DELIVERY

All unclassified deliverables or correspondence shall be submitted electronically to the following website location: <https://portal.fas.gsa.gov/>

Unclassified deliverables or correspondence shall be delivered to the CO, CS, and COR at the following email addresses:

ATTN: Erin.Greninger@gsa.gov;
Elizabeth.Steiner@gsa.gov;
Mignon.Stephens@gsa.gov;
HuyD.Le@gsa.gov

F.6 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR via a Problem Notification Report (PNR) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 TASK ORDER ADMINISTRATION

Contracting Officer:

Erin Greninger

GSA FAS NCR

301 7th Street, SW

Washington, D.C. 20407

Telephone: (b) (6)

Email: Erin.Greninger@gsa.gov

Contracting Specialist:

Elizabeth Steiner

GSA FAS NCR

3017th Street, SW

Washington, D.C. 20407

Telephone: (b) (6)

Email: Elizabeth.Steiner@gsa.gov

Program Manager:

Mignon Stephens

GSA FAS NCR

3017th Street, SW

Washington, D.C. 20407

Telephone: (b) (6)

Email: Mignon.Stephens@gsa.gov

Contracting Officer's Representative:

Huy D. Le

GSA NewPay

1800 F Street, NW

Washington, DC 20036

Telephone: (b) (6)

Email: Huyd.Le@gsa.gov

G.1.1 CONTRACTING OFFICER (CO)

1. The Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds. No person other than the Contracting Officer can make any changes to the terms, conditions, general provisions, or other stipulations of this contract.

2. The Contracting Officer is the only person with the authority to act as agent of the Government under this contract. Only the Contracting Officer has authority to:
 - a. Direct or negotiate any changes in the statement of work;
 - b. Modify or extend the period of performance;
 - c. Change the delivery schedule;
 - d. Authorize reimburse to the Contractor of any costs incurred during the performance of this contract; and
 - e. Otherwise change any terms and conditions of this contract.
3. No information other than that which may be contained in an authorized modification to this contract, duly issued by the Contracting Officer, which may be received from any person employed by the US Government, other otherwise, shall be considered grounds for deviation from any stipulation of this contract.
4. The Government may unilaterally change its CO designation, after which it will notify Contractor in writing of such change.

G.1.2 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The CO shall appoint a COR in writing through a COR Appointment Letter. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and/or price of the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the TO.

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (JAN 2017), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

1. TO Number: (from GSA Form 300, Block 2)
2. Paying Number: (ACT/DAC NO.) (From GSA Form 300, Block 4)
3. Project Number: (TBD: ID number)
4. Project Title: Loan Accounting System (LAS) Operations and Maintenance Support

The contractor shall submit invoices as follows:

1. Utilize AAS's electronic Assisted Services Shared Information System (ASSIST) to submit invoices;

2. Manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs;
3. Submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link): <https://portal.fas.gsa.gov>;
4. Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA AAS or the GSA Finance Center; and
5. Provide invoice backup data, as an attachment to the invoice, in accordance with the TO type, including details such as labor categories, rates, and quantities of labor hours per labor category.

The COR may require the contractor to submit a written “hardcopy” invoice with the client’s certification prior to invoice payment. A paper copy of the invoice is required for a credit. The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at: AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the CO, CS, and the COR for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR Part 32.9 and GSAM 532.9.

Each TO shall be addressed separately in the invoice submission (if applicable). The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

The contractor shall report the following metadata at a minimum:

1. TO Number
2. Contractor Invoice Number
3. Contractor Name
4. Point of Contact Information.
5. Current period of performance.
6. Amount of invoice that was subcontracted.

The amount of the invoice that was subcontracted to a small business shall be made available upon request.

The contractor shall invoice monthly on the basis of hours incurred for the T&M CLINs (if applicable). The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date:

1. Employee name (current and past employees).
2. Employee company.
3. Exempt or non-exempt designation.
4. Service Occupational Classifications (SOC) number.
5. Employee labor category.
6. Current monthly and total cumulative hours worked.
7. Direct Labor Rate.
8. Corresponding negotiated ceiling rate
9. Effective hourly rate (e.g., cumulative costs/cumulative hours).
10. Current approved billing rate percentages in support of costs billed.
11. Labor adjustments from any previous months (e.g., timesheet corrections).

G.3.1 RESERVED

G.3.2 TRAVEL

5 CFR 330.604(e) states “Local commuting area means the geographic area that usually constitutes one area for employment purposes as determined by the agency. It includes any population center (or two or more neighboring ones) and the surrounding localities in which people live and can reasonably be expected to travel back and forth daily to their usual employment.” There is no longer a standard mileage used for long-distance travel. The 50 mile rule has been removed from the FTR. Use over 50 miles to define long-distance travel unless changed by the CO.

The JTR, FTR, and DSSR are references for what is reasonable to be invoiced. Due to the travel reimbursement changes in the National Defense Authorization Act, IPTs should review with the client how long-term TDY and per diem will be reimbursed and add language to the solicitation request accordingly.

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

1. Federal Travel Regulation (FTR) - prescribed by GSA, for travel in the contiguous United States (U.S.).
2. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
3. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.
4. The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the FTR. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.
5. CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:
 - a. Travel Authorization Request number or identifier, approver name, and approval date.
 - b. Current invoice period.
 - c. Names of persons traveling.
 - d. Number of travel days.
 - e. Dates of travel.
 - f. Number of days per diem charged.
 - g. Per diem rate used.
 - h. Total per diem charged.
 - i. Transportation costs.
 - j. Total charges.
 - k. Explanation of variances exceeding ten percent of the approved versus actual costs.
 - l. Indirect handling rate.
 - m. All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's DCAA cost disclosure statement.

G.4 TASK ORDER AWARD CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the contractual period of performance if the contractor does not provide final DCAA rates by that time.

G.5 CLARIFICATIONS

1. Change management and communication external to GSA will be the responsibility of the Government. The vendor is not expected to work directly with the Business Standards Council or other governance bodies external to GSA. The vendor will be responsible for providing status and reporting information which will typically be included as part of the status reporting identified in this task order.
2. The vendor will create the IV&V plan. The vendor does not include third-party IV&V costs to conduct the IV&V.
3. The NARA requirements for data retention are inclusive of the subscription cost which is not within the scope of this task order.
4. It is the Government's understanding that a commercial payroll SaaS solution will have a set of standard interfaces applicable across its client base. The Government will not be responsible for these interfaces.
5. Parallel testing for the purpose of comparing results between the SaaS and legacy systems using live production data is not within the scope of this task order.
6. The Government does not require the vendor to provide external change management activities during the build under this task order.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this Award.

Definition. "Personnel" means employees of the contractor, or any subcontractor(s), affiliates, joint venture partners, or team members, and consultants engaged by any of those entities.

The personnel specified below are considered to be essential to the work being performed under this TO. Prior to diverting any of the specified individuals to other projects, the contractor shall notify the Contracting Officer reasonably in advance and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the program. No diversion shall be made by the contractor without the written consent of the Contracting Officer.

CARAHSOFT KEY PERSONNEL	
Name	Position
(b) (6)	Project Manager
(b) (6)	Functional SME
(b) (6)	Technical SME

The Government requires that Key Personnel be assigned for the duration of the Award.

H.1.1 PROJECT MANAGER (PM)

The contractor shall identify a Project Manager (PM) by name who shall provide management to include: organizing, planning, coordinating, scheduling, tracking and executing the activities required to achieve the requirements (as defined in Section C). The PM is also responsible for the management of resources and reporting of the project status. The PM will serve as the government’s primary point of contact for all issues dealing with the successful deliverables (as defined in Section F) and leadership of the execution of this Award.

H.1.2 FUNCTIONAL SUBJECT MATTER EXPERT (SME)

The contractor shall identify a Functional SME by name who has the relevant payroll and implementation experience to support the PM in the planning, analysis, evaluation, and testing of the SaaS solution. The Functional SME will lead or advise on functional activities needed to achieve the business capabilities requirements (as defined in Section C) and their impacts on the government’s processes and operations.

H.1.3 TECHNICAL SUBJECT MATTER EXPERT (SME)

The contractor shall identify a technical subject matter expert (SME) with a broad range of technical skills and experience necessary to support and advise the project manager on technical aspects required for this task order. Technical areas of expertise or experience dealing with areas such as configuration of the SaaS solution, data management and data interfaces, and IT security. The Technical SME will be the primary lead to work with the government's technical SMEs to achieve the requirements (as defined in Section C).

H.1.4 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the Award, the contractor shall notify the CO and COR of the existing Award. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the CO and the COR determines that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-8, Default (*Fixed-Price Supply and Service*).

H.2 SECURITY REQUIREMENTS

The services identified in this TO will adhere to the rules, regulations, laws, standards, and conventions identified by GSA as well as within the Federal Government. The GSA Agency Security Requirements are in Attachment H. These standards and guidelines are mandatory.

H.3 INFORMATION ASSURANCE

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense and is an event of default.

H.4 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.4.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

1. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
2. The contractor is required to complete and sign an OCI Statement (Section J). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this TO, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
3. If a contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
4. In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
5. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the TO awarded.

H.4.2 NON-DISCLOSURE REQUIREMENTS

All employees working under the task order, including all subcontractor employees at any tier, must sign the NDA form set forth in Section J, Attachment L.

The contractor shall ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

1. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
2. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO award or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be

liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.5 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

FTR - Prescribed by GSA, for travel in the contiguous U.S.

H.6 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a Travel Authorization Request (TAR) for Government review and approval. Long-distance travel will be reimbursed at cost of travel comparable with the FTR.

Requests for travel approval shall:

1. Be prepared in a legible manner.
2. Include a description of the travel proposed including a statement as to purpose.
3. Be summarized by traveler.
4. Identify the TO number.
5. Identify the CLIN associated with the travel.
6. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.7 DATA RIGHTS

(a) The Government shall have unlimited rights in all data first produced in the performance of this task order, including without limitation all deliverables listed in the deliverables table in section F.2, in accordance with the FAR clause at 52.227-14, Rights in Data – General (May 2014), which is hereby incorporated in this task order.

(b) The Government understands that the commercial SaaS solution that will be provided in furtherance of this Award as described in Section C. and as contemplated in the applicable CLINs in Section B (included with final Award) may be subject to one or more commercial agreements, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). For purposes of this Award, the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14 and “Commercial Supplier Agreements” within the meaning of the GSAR

clause at 48 CFR 552.212-4, Contract Terms and Conditions – Commercial Items (FAR Deviation)(Feb 2018).

The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this Award. The contractor shall provide all applicable Supplier Agreements to the CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government:

1. Access and use by support contractors, including a successor contractor upon termination or expiration of this Award;
2. Access and use by other Federal agencies;
3. Transfer to a different data center and/or a successor contractor's cloud; and
4. The creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above.

The above rights constitute “other rights and limitations” as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

(c) Rights in Government-provided data that will populate and be processed by the SaaS solution shall be as set forth in sections 1.8 and 1.12 of Attachment H.

H.8 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the CO/COR.

H.9 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

I.1 – TASK ORDER CLAUSES

I.1 All applicable clauses per the BPA will apply to this TO.

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. The full text of a clause may be accessed electronically at the FAR <https://www.acquisition.gov/far> and GSAM website: <https://acquisition.gov/browsegsam>

I.2 FEDERAL ACQUISITION REGULATION (FAR) CLAUSE INCORPORATED BY REFERENCE

FAR	TITLE	DATE
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2019
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2019
52.212-3	Offeror Representations and Certifications-Commercial Items	Oct 2018
52.239-1	Privacy or Security Safeguards	AUG 1996

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.204-70	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2019

552.212-4	Contract Term and Conditions – Commercial Items (FAR Deviation)	FEB 2018
552.232-25	Prompt Payment	NOV 2009
552.239-70	Information Technology Security Plan and Security Authorization	JUN 2011
552.239-71	Security Requirements for Unclassified Information Technology Resources	JAN 2012
552.203-71	Restriction on Advertising	SEP 1999
552.211-73	Marking	FEB 1996
552.215-70	Examination of Records by GSA	JUL 2016
552.237-71	Qualifications of Employees	MAY 1989

I.3.1 GSAM CLAUSES INCORPORATED BY FULL TEXT

GSAM 552.212-71 CONTRACT TERMS AND CONDITIONS APPLICABLE TO GSA ACQUISITION OF COMMERCIAL ITEMS (JUNE 2016)

Contract Terms and Conditions Applicable to GSA Acquisition of Commercial Items (Jul 2003)

(a) The Contractor agrees to comply with any clause that is incorporated herein by reference to implement agency policy applicable to acquisitions of commercial items or components. The clause in effect based on the applicable regulation cited on the date the solicitation# ID11190033 is issued applies unless otherwise stated herein.

SECTION J - LIST OF ATTACHMENTS

ATTACHMENT	TITLE	Location
A	Business Capabilities and Data Standards	BPA
B	Technical Capabilities	BPA
C	Pay Plans	Attachment
D	Interface Requirements	Attachment
E	Reserved	
F	Data Standards and Architecture	Included (1 pg.)
G	Monthly Status Report (MSR) Template	Included (2 pgs.)
H	Agency Security Requirements	Included (32 pgs.)
I	Functional Requirements	Included (8 pgs.)

ATTACHMENT F - DATA STANDARDS AND ARCHITECTURE

The Office of Personnel Management (OPM), Human Resources Line of Business (HRLOB) released the V1.1 Federal HC Data Standard, December 21, 2018. The Standard is published to the OPM HRLOB OMB Max webpage at <https://community.max.gov/display/HumanCapital/Products> .

Access to OMB Max requires a “.mil” or “.gov” email address or sponsorship by government employee with an active account on max.gov. The HRLOB webpage is publicly accessible.

ATTACHMENT G - MONTHLY STATUS REPORT

Contract No. ID _____

MONTHLY STATUS REPORT

Month day, 20xx through Month day, 20xx

on

Project Title

Contractor Name

to

General Service Administration

Assisted Acquisition Services

301 7th Street, S.W., Washington, D.C. 20410

Report submittal date

Author , Contact Info

The monthly report shall consist of:

Table of Contents:

Project Objective

Executive Summary

Progress

Overall Progress.

Management and Administrative Update (Include Title and WBS prior to written narrative)

WBS 1.x.x.xa Technical Progress

Proposed Work

Appendix A

Appendix B

Project Objective:

Executive Summary:

Summary of work done this reporting period:

Immediate issues to be addressed in the next reporting period:

Issue 1

Issue 2

Issue 3

Progress (Include Title and WBS prior to written narrative):

Part A. Overall Progress

Part B. Management and Administrative Update WBS X.X

Part C. Technical Progress

Part D. Proposed Work

Appendix A

Appendix B

ATTACHMENT H - AGENCY SECURITY REQUIREMENTS

General Services Administration, Quality Services Management Office (QSMO) – NewPay SaaS Solution

Introduction

The U.S. General Services Administration (GSA) must provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by GSA, another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, information systems used or operated by an agency or other organization on behalf of an agency.

Office of Management and Budget (OMB) Memorandum M-14-04 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in FISMA of 2014, OMB’s implementing policies including OMB Circular A-130 and guidance and standards from the National Institute of Standards and Technology (NIST).

Scope

This guide provides security and privacy requirements for the GSA information system types outlined below:

- **Cloud Information Systems.** Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. Requires FedRAMP.
- **Mobile Application.** A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.

1. Cloud Information Systems – IT Security and Privacy Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for **Moderate** impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **Moderate** impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, “*Security and Privacy Controls for Federal Information Systems*”

and Organizations” (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

1.1. Assessment and Authorization

1.2. Assessment of the System

1.2.1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System’s FIPS PUB 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at <https://www.fedramp.gov/>:

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- Contingency Plan (CP)
- Contingency Plan (CP) Test Results
- Plan of Action and Milestones (POA&M)
- Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

1.2.2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system’s security posture in accordance with the FedRAMP Continuous Monitoring Plan.

1.2.3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and

Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

1.2.4. The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

1.2.5. Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

1.2.6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.

1.2.7. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

1.3. Authorization of the System

1.3.1. If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website: <https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=Compliant> GSA will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the

agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.

1.3.2. If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

1. Operate on an CSP IaaS environment that is FedRAMP authorized; AND
2. Be listed as FedRAMP In Process on the FedRAMP Website -
<https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=In%20Process>

OR be listed as FedRAMP Ready on the FedRAMP website -

<https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=FedRAMP%20Ready>

3. Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment Review completed by a [FedRAMP 3PAO](#) following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, GSA will terminate the contract.
4. If requirements a-c, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the GSA Moderate Impact SaaS Solutions process as described in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk*." The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA Moderate Impact SaaS A&A process. Without a FedRAMP authorization within 1 year of contract award; GSA will not be able to use the product for the option years and shall terminate the contract.

1.3.3. CSP shall ensure the essential security controls listed in the table below are implemented. CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H

MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	PKI Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H
SC-28 (1)	Protection of Information at Rest Cryptographic Protection	M, H

SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

1.4. Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

1.4.1. Quarterly OS, web, and database vulnerability scans (deliverable shall include raw results and findings shall be included in the POA&M document);

1.4.2. Quarterly Plan of Action and Milestones (POA&M);

1.4.3. Annual A&A Package updates including the System Security Plan, Contingency Plan, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

1.5. Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, “*GSA Information Technology (IT) Security Policy*,” and GSA Order CIO P 2181.1, “*HSPD-12 Personal Identity Verification and Credentialing Handbook*.” GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as “Applicant”) determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer’s (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

1.6. Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, "*Guidelines for Media Sanitization.*" The destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

1.7. Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as SBU information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

1.8. Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

1.9. Personally Identifiable Information

Personally identifiable information (PII) is in the scope of acquisition and PII is expected to be stored in the vendor's cloud solution. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

PII (should it come into scope) will require that the vendor's cloud solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

1.10. Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

1.11. Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

1.12. Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

1.13. Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

1.14. GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

1.15. Additional Stipulations

1.15.1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."

1.15.2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

1.15.3. The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

1.15.4. The contractor shall comply with any additional FedRAMP privacy requirements.

1.15.5. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

- a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
- b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
- c. The program of inspection shall include, but is not limited to:
 - Authenticated and unauthenticated operating system/network vulnerability scans
 - Authenticated and unauthenticated web application vulnerability scans
 - Authenticated and unauthenticated database application vulnerability scans
 - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

1.15.6. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

1.15.7. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits the use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

1.15.8. The Contractor shall comply and ensure Government compliance with any law, regulation or Executive Order prohibiting the use of any hardware, software or services, to

include Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.

1.16. References

[Guide to Understanding FedRAMP](#)
[FedRAMP Cloud Computing Documents](#)
[FedRAMP Templates](#)

1.17. Required IT Security and Privacy Policies, Laws and Regulations

The contractor's work, services and deliverables shall at all times comply with each of the following standards. In cases where standards apply by their terms to Government agencies, the contractor's work shall comply as if it were the agency.

Federal Laws and Regulations:

The contractor shall comply with all applicable Federal Laws and Regulations.

- [40 U.S.C. 11331](#), “Responsibilities for Federal Information Systems Standards”
- [FISMA of 2014](#), “The Federal Information Security Modernization Act of 2014”
- [HSPD 12](#), “Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors”
- [OMB Circular No. A-130](#), “Managing Information as a Strategic Resource”
- [OMB M-08-23](#), “Securing the Federal Government’s Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)”
- [OMB M 14-03](#), “Enhancing the Security of Federal Information and Information Systems”
- [OMB M-10-23](#), “Guidance for Agency Use of Third-Party Websites and Applications”
- [OMB M-15-13](#), “Policy to Require Secure Connections across Federal Websites and Web Services”
- [OMB M-17-12](#), “Preparing for and Responding to a Breach of Personally Identifiable Information”
- [Privacy Act of 1974](#), “5 USC, § 552a”
- [OMB Memoranda](#), location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) usage is mandatory.

- [FIPS PUB 199](#), “Standards for Security Categorization of Federal Information and Information Systems”
- [FIPS PUB 200](#), “Minimum Security Requirements for Federal Information and Information Systems”
- [FIPS PUB 140-2](#), “Security Requirements for Cryptographic Modules”
- [NIST SP 800-18, Revision 1](#), “Guide for Developing Security Plans for Federal Information Systems”

- [NIST SP 800-30, Revision 1](#), “Guide for Conducting Risk Assessments”
- [NIST SP 800-34, Revision 1](#), “Contingency Planning Guide for Federal Information Systems”
- [NIST SP 800-37, Revision 1](#), “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach”
- [NIST SP 800-47](#), “Security Guide for Interconnecting Information Technology Systems”
- [NIST SP 800-53, Revision 4](#), “Security and Privacy Controls for Federal Information Systems and Organizations”
- [NIST SP 800-53A, Revision 4](#), “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans”
- [NIST SP 800-63-3](#), “Digital Identity Guidelines”
- [NIST SP 800-122](#), “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”
- [NIST SP 800-137](#), “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”
- [NIST SP 800-161](#), “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”
- [NIST SP 500-267](#), “A Profile for IPv6 in the U.S. Government”

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- [GSA Order CIO 1878.1](#), “GSA Privacy Act Program”
- [GSA Order CIO 1878.2](#), “Conducting Privacy Impact Assessments (PIAs) in GSA”
- [GSA Order CIO 2100.1](#), “GSA Information Technology (IT) Security Policy”
- [GSA Order CIO 9297.2](#), “GSA Information Breach Notification Policy”

The contractor shall comply with the following GSA policies listed below when inside a GSA building or inside a GSA firewall.

- [GSA Order CIO 2100.3](#), “Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities”
- [GSA Order 9732.1 ADM P](#), “Suitability and Personnel Security”

The GSA policies listed in this paragraph must be followed, if applicable.

- [GSA Order CIO 2103.1](#), “Controlled Unclassified Information (CUI) Policy”
- [GSA Order CIO 2104.1](#), “GSA Information Technology (IT) General Rules of Behavior”
- [GSA Order CIO 2182.2](#), “Mandatory Use of Personal Identity Verification (PIV) Credentials”

GSA Procedural Guides:

The contractor shall comply with all applicable GSA IT Security Procedural Guides. GSA’s Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit [GSA.gov](#). If a non-publicly available guide is needed, contact the contracting officer who will coordinate with GSA Office of the Chief Information Security Officer to determine if it can be made available.

2. Mobile Application - IT Security and Privacy Requirements

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, “*GSA Information Technology (IT) Security Policy*” and GSA IT Security Procedural Guide 12-67, “*Securing Mobile Devices and Applications*,” or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

2.1. General Mobile Application Guidelines

1. The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. GSA currently uses MAAS 360.

1. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure (SOP) before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
2. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.

- The contractor shall provide detailed process and code documentation.
- The contractor shall provide App features documentation.
- The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, “*Securing Mobile Devices and Applications*,” or current version.

2.2. Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, “*Securing Mobile Devices and Applications*,” which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user’s PC. However, as mobile app development has grown, a more sophisticated approach involves developing applications

specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple iTunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

2.3. Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple iTunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation.
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation.
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

- [Apple App Review guidelines](#)
- [Google Play Store Developer Policy Center](#)

2.4. GSA Privacy Requirements

Personally identifiable information (PII) is in the scope of the acquisition and PII is expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App. Instructions for the PTA and PIA forms can be found at <https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia>.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement when bracketed sections are completed. A completed example is available at

<https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research>
[ch](#).

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information is authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g. name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert App name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

2.5. GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA FISMA system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk,"* is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).
- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, *"Securing Mobile Devices and Applications"* and the release process documented in this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.

- All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for developing OWASP is outlined below:

[OWASP Mobile Security Testing Guide](#)

[OWASP Mobile Security Project Home Page](#)

[OWASP Security Testing Guidelines for Mobile Apps](#)

- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
- Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security Plan for the system they support.
- Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review in accordance with the GSA-IT Procedural Guide: CIO-IT Security-12-67, "*Securing Mobile Devices and Applications*" must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

2.6. Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license

to reproduce all works (including technical and scientific articles) produced during this task order.

2.7. Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

2.8. GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term “proprietary information” means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

2.9. Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1 – “*GSA Information Technology (IT) Security Policy*” and GSA Order CIO P 2181.1 – “*HSPD-12 Personal Identity Verification and Credentialing Handbook*.” GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as “Applicant”) determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer’s (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and

access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

2.10. Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.
3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
 - i. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical

capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

The Contractor shall comply with Section 1634 of [Public Law 115-91](#) that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

3. Incident Response

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*" and GSA IT Security Procedural Guide 01-02, "*Incident Response (IR)*," or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

3.1 References

[IT Security Procedural Guide: Incident Response \(IR\), CIO-IT Security-01-02](#)

ATTACHMENT I - FUNCTIONAL REQUIREMENTS

LABOR DISTRIBUTION PAYROLL REQUIREMENT: As part of HCM.120 Compensation Management (Payroll Administration) from Attachment A (Business Capabilities and Data Standards), “Track and process payroll calculations and adjustments that cross fiscal years, calendar years, and/or other accounting period and provide appropriate data to the core financial and other information systems”. The Contractor solution shall provide labor tracking and cost allocation functionality to distribute and transfer payroll expenses to general ledger(s), labor codes, lines of accounting, projects, tasks/activities (e.g. buildings), or a combination. Individual employee salaries can be paid through multiple funding sources. Payroll amounts (labor costs) need to be allocated for all time that is recorded on time cards with the capability to validate accounting codes and to adjust distribution based upon payroll standards and financial management business rules. The Contractor solution shall accept interfaced data or generate a data set to redistribute labor costs to or from a combination of accounting, labor, function and project category codes.

CUSTOMER or USER EXPERIENCE: The Contractor shall apply human centered design methods that are a practical and repeatable approach to arriving at innovative solutions.

OUTPUTS (REPORTS AND FILES): The Contractor shall configure and/or develop, maintain, and execute outputs, reports, and files to meet the business and technical needs of the Government and customer agencies. The Contractor’s solution shall provide a reporting capability that provides relevant and timely reports to specific user roles. The reporting capability should facilitate the development of reports based on payroll categories such as:

- Accounting Distributions
- Pay Deductions and Garnishments
- Pay Types
- Year to Date and Year End Summaries
- Labor Cost Allocation and Tracking
- Leave Types and Accruals
- Retirement Reports

DATA RIGHTS: The federal government will retain unrestricted rights to all government data and maintain the right to request full copies, at any time, in a format that is readily accessible through predominant industry and/or open data formats to which the federal government agencies agree. Data will be provided at no additional cost to the federal government. The Contractor shall provide National Archives and Records Administration (NARA) official records housed and maintained by the SaaS provider to Federal agencies upon request no more than 30 days from initial request. Information regarding payroll records can be found at NARA’s website. Ad hoc requests for Government data must be available within (5) five business days.

DATA CURRENCY AND VALIDITY

The Contractor shall develop, maintain, and execute processes and procedures to ensure the currency and validity of Master Data/Enterprise Reference Data, configurations, business rules, and other elements of the solutions. These elements include but are not limited to pay plans, pay tables, locality tables, pay and leave policies, and regulations.